

Risk Reduction, Safety Allocation And Safety Requirements Specification

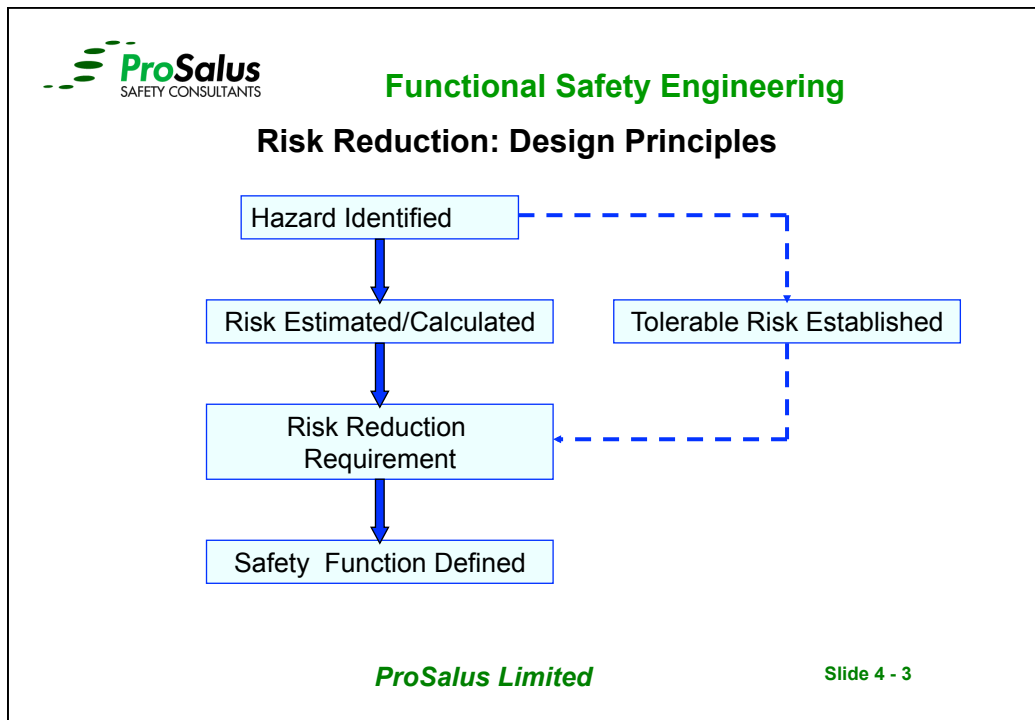
Slide 4 - 1


Risk Reduction

- At this point we know
 - We have identified the hazards
 - The cause / consequences pairs of the hazards
 - The likelihood or frequency of the hazards
- **Now we need to ask ourselves**
 - What is our Risk Target / Tolerability Criteria
 - Do we need to reduce the risk to make it As Low As Reasonably Practicable “ALARP”?
 - If so how much risk reduction is required?
 - Do we need a SIF to fill the gap to meet the Risk Target?

ProSalus Limited

Slide 4 - 2



 **Functional Safety Engineering**

Risk Perception

- **There are different levels of risk:**
 - **High Consequence Low Frequency**
 - E.g. being struck by lightning 14 million to 1
 - **Low Consequence High Frequency**
 - E.g. office work – paper cuts etc
- Beware low frequency / high Consequence events
 - **Tolerable Risk**
 - Lies between negligible and unacceptable
 - The ALARP Region also requires consideration of reasonable practicability, established good practice & cost / Benefit Analysis
 - HSE – “Reducing Risks, Protecting People” (R2P2) and website for additional ALARP & CBA Guidance

ProSalus Limited Slide 4 - 4



Functional Safety Engineering

Individual Risk

Individual risk is the risk experienced by a single individual in a given time period. It reflects the severity of the hazards and the amount of time the individual is in proximity to them. The number of people present does not significantly affect it.

Individual risk is defined formally by the IChemE (1992) as the frequency at which an individual may be expected to sustain a given level of harm from the realisation of specified hazards. It is usually taken to be the risk of death, and usually expressed as a risk per year.

ProSalus Limited

Slide 4 - 5



Functional Safety Engineering

Fatal Accident Rate - FAR

Individual risks for workers are commonly expressed as a fatal accident rate (FAR), which is the number of fatalities per 10^8 exposed hours. FARs are typically in the range 1-30, and are more convenient and readily understandable than individual risks per year, which are typically in the range 10^{-5} - 10^{-3} . The number of 10^8 exposed hours is roughly equivalent to the number of hours at work in 1000 working lifetimes. The FAR measure was developed to describe onshore occupational risks, which only apply during working hours. Hence, in onshore studies, 'exposed hours' is taken to mean 'hours at work', and the FAR is defined as:

$$\text{Onshore FAR} = \frac{\text{Fatalities at work} \times 10^8}{\text{Person hours at work}}$$

ProSalus Limited

Slide 4 - 6

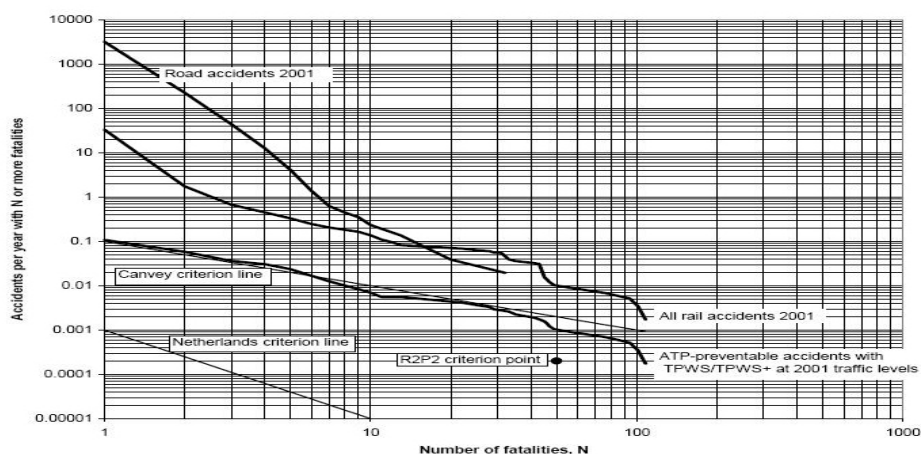
Societal Risk

Societal risk is the risk experienced in a given time period by the whole group of personnel exposed. It reflects the severity of the hazard and the number of people in proximity to it. It is usually taken to refer to the risk of death, and usually expressed as a risk per year.

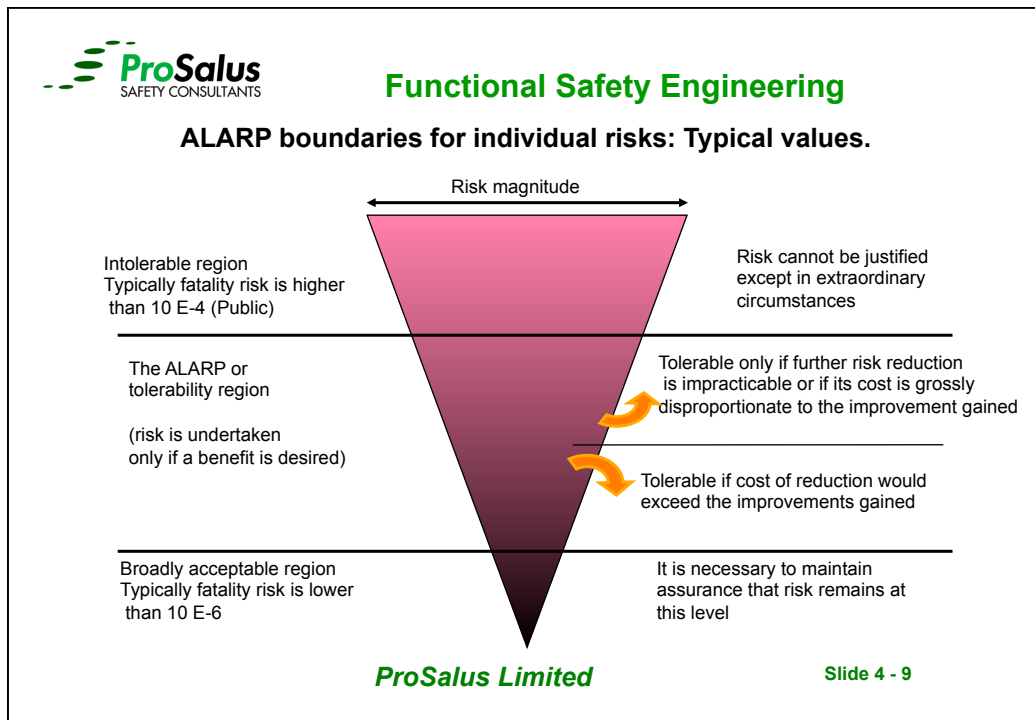
Societal risks are defined by the IChemE (1992) as the relationship between the frequency and the number of people suffering a given level of harm from the realisation of specified hazards. This definition excludes single-figure measures such as annual fatality rate (see below) and so the wider definition above is preferred. The term 'societal risk' is also sometimes taken to refer to members of the public


Societal risks are generally expressed in the form of FN curves showing the relationship between the cumulative frequency (F) and number of fatalities (N)

Figure 4: Transport FN-curves for 2001 and FN-criteria



Example FN – Curve Slide courtesy of UK HSE



 **Functional Safety Engineering**

Government Tolerable - Risk Criteria Summary

	Maximum acceptable risk to the public
UK	1×10^{-4}
Hong Kong	1×10^{-5}
Netherlands	1×10^{-6}
Australia	1×10^{-6}

ProSalus Limited Slide 4 - 10



Functional Safety Engineering

As Low As Reasonably Practicable (HSE)

- The concept of “Reasonably Practicable” is fundamental to the setting of Health& Safety goals rather than being prescriptive.
- In most cases can be achieved by implementing existing “good practice” e.g. IEC 61511 for Safety Instrumented Systems
- For high hazard scenarios a more formal decision making technique is required, that could include event trees, fault trees, fire and gas modeling possibly compiled as a safety case or safety report that includes cost benefit analysis, sensitivity analysis and optioneering
- Reasonably Practicable means (Edwards v NCB [1949]) weighing the risk against the sacrifice needed to further reduce it always weighting the decision in favour of H&S because the presumption is always that the risk reduction measure should be implemented

ProSalus Limited

Slide 4 - 11



Functional Safety Engineering

Cost Benefit Analysis (HSE)

- Benefits can include: reduction in risk to workers & the public; cost of avoidance of contamination, environmental damage, site evacuation; deployment of emergency services
- Typical costs of prevention of H&S impact on people are (HSE)
 - Fatality - £1,336, 800 (x2 for cancer)
 - Permanent injury - £207,200
 - Serious injury - £20,500
 - Slight - £300
- Typical Disproportion factors (HSE) “rules of thumb”
 - 3 for risks to workers
 - 2 for low risks to members of the public
 - 10 for high risk scenarios i.e. multiple fatalities

ProSalus Limited

Slide 4 - 12



Functional Safety Engineering

CBA Worked Example (HSE)

- Consider a chemical plant with a process that if it were to explode could lead to:
 - 20 fatalities
 - 40 permanently injured
 - 100 seriously injured
 - 200 slightly injured
- The rate of this explosion is 1 in 100,000 per year.
- The plant has an estimated lifetime of 25 years.
- How much could the company reasonably spend to eliminate (reduce to zero) the risk from the explosion?
- If the risk of explosion were to be eliminated the benefits can be assessed to be:

▪ Fatalities:	20	x £1,336,800	x 1x10 ⁻⁵	x 25 yrs	= £6684
▪ Permanent injuries:	40	x £207,200	x 1x10 ⁻⁵	x 25 yrs	= £2072
▪ Serious injuries:	100	x £20,500	x 1x10 ⁻⁵	x 25 yrs	= £512
▪ Slight Injuries:	200	x £300	x 1x10 ⁻⁵	x 25 yrs	= £5
▪ Total benefits =					= £9,283
- The sum of £9,283 is the estimated benefit of eliminating the major accident explosion at the plant on the basis of avoidance of casualties. (This does not include discounting or take account of inflation)
- For a measure to be deemed not reasonably practicable, the cost has to be grossly disproportionate to the benefits.
- This is taken into account by the disproportion factor (DF). In this case, the DF must reflect that the consequences of the explosion are high. Therefore based on HSE guidance a DF of 10 is considered reasonable
- Therefore it would be reasonably practicable to spend up to somewhere in the region of **£93,000 (£9300 x 10)** to eliminate the risk of an explosion on the plant.

ProSalus Limited

Slide 4 - 13



Functional Safety Engineering

Overview Of Formal Risk Analysis Techniques

ProSalus Limited

Slide 4 - 14



Functional Safety Engineering

Risk Management can be applied in three ways

- Reduce the consequences to an acceptable level, or
- Reduce the frequency to an acceptable level, or
- Reduce the overall risk to an acceptable level

Risk Analysis Techniques

- **Risk Analysis** is the systematic use of available information to identify hazards and to estimate the risk to individuals, groups (societal), assets or the environment
- **Risk Estimation** is the process used to produce a measure of the level of risk for the hazard being analysed and consists of:
 - Frequency Analysis
 - Consequence Analysis
- **Risk Evaluation** is the judgement as to whether the risk is tolerable taking into account a countries risk criteria and other factors such as environmental and socio-economic aspects

ProSalus Limited

Slide 4 - 15



Functional Safety Engineering

Typical Risk Analysis Techniques used in the Process Industry

- Event Tree Analysis
- Failure Mode and Effect Analysis & Criticality Analysis
- Fault Tree Analysis
- Hazard and Operability Studies (HAZOP)
- Human Reliability Analysis
- Preliminary Hazard Analysis (HAZID)
- Reliability Block Diagrams
- Consequence Models
- Sneak Analysis

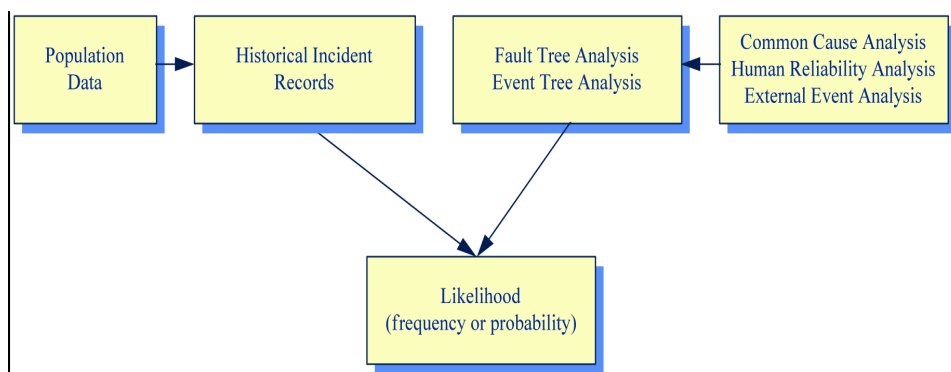
ProSalus Limited

Slide 4 - 16

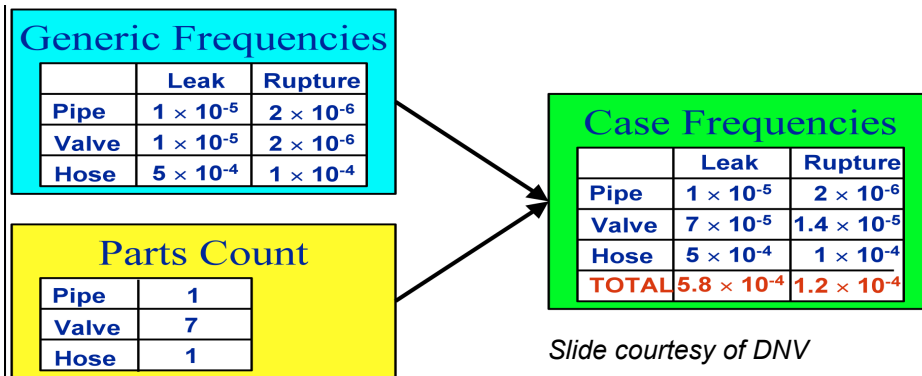
Frequency Analysis

- Used to estimate the likelihood of each identified hazardous event
- Three approaches are commonly used to estimate frequencies:
 1. Use relevant historical failure data e.g. OREDA, AIChem, Faradip
 2. Frequency of event derived from analytical techniques e.g. ETA, FTA
 3. Use of expert judgement

Frequency Analysis (DNV)



Failure Case Frequency Calculation Method Based on Historical data Method



ProSalus Limited

Slide 4 - 19

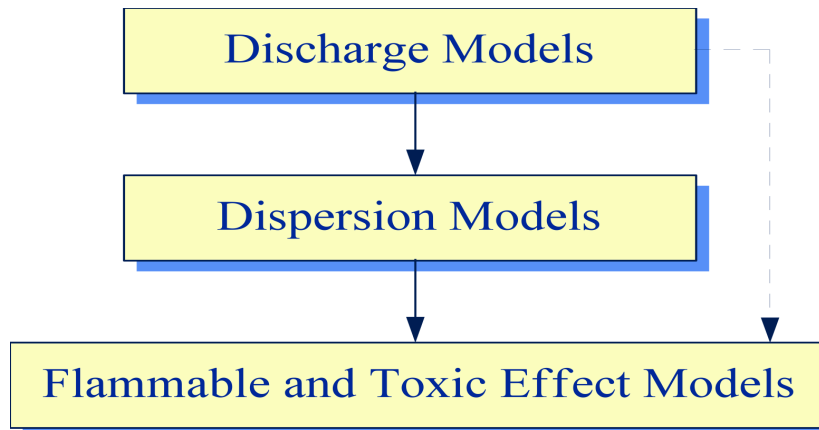
Consequence Analysis

- Used to estimate the likely impact on individuals, populations (societal), property or the environment should the undesired event identified during hazard identification occur
- Usually an estimate of the number of people (receptors), located in different environments at different distances from the source of the event
 - that might be either killed, injured or seriously affected by the event
- Events usually comprise of
 - Release of toxic materials
 - Fires
 - Explosions
 - Projectiles
- Further information - Guidelines for Chemical Process QRA CCPS publication ISBN 0 8169 0720 X

ProSalus Limited

Slide 4 - 20

Consequence Analysis

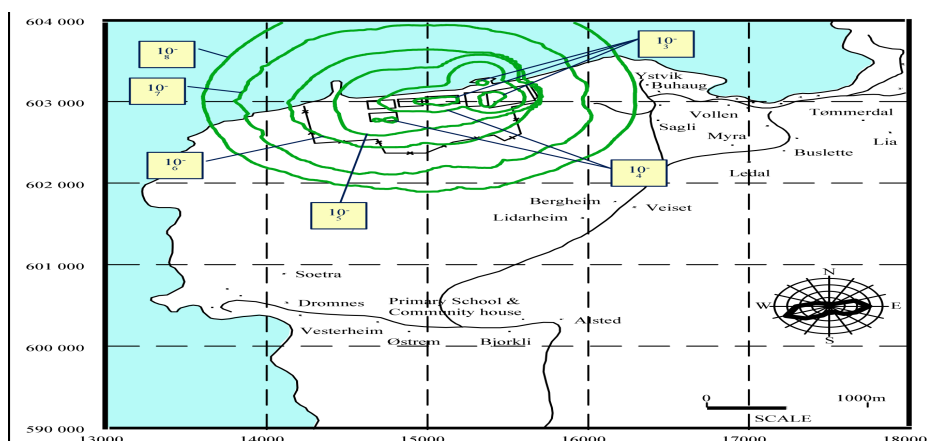


Slide courtesy of DNV

ProSalus Limited

Slide 4 - 21

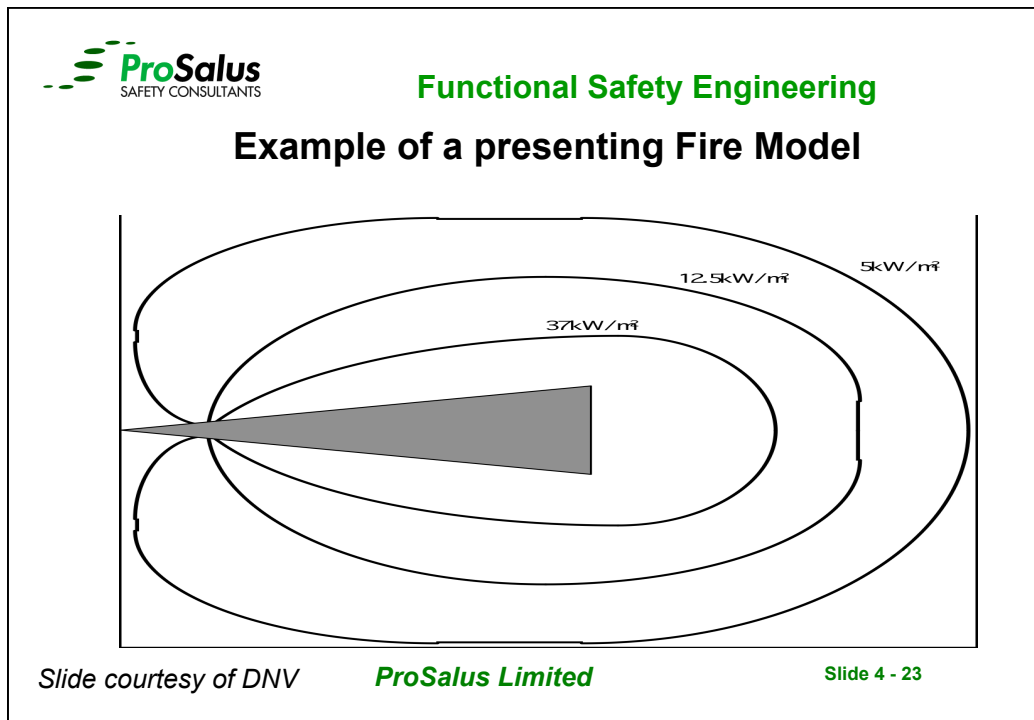
Example of presenting Risk Contours




Slide courtesy of DNV

ProSalus Limited

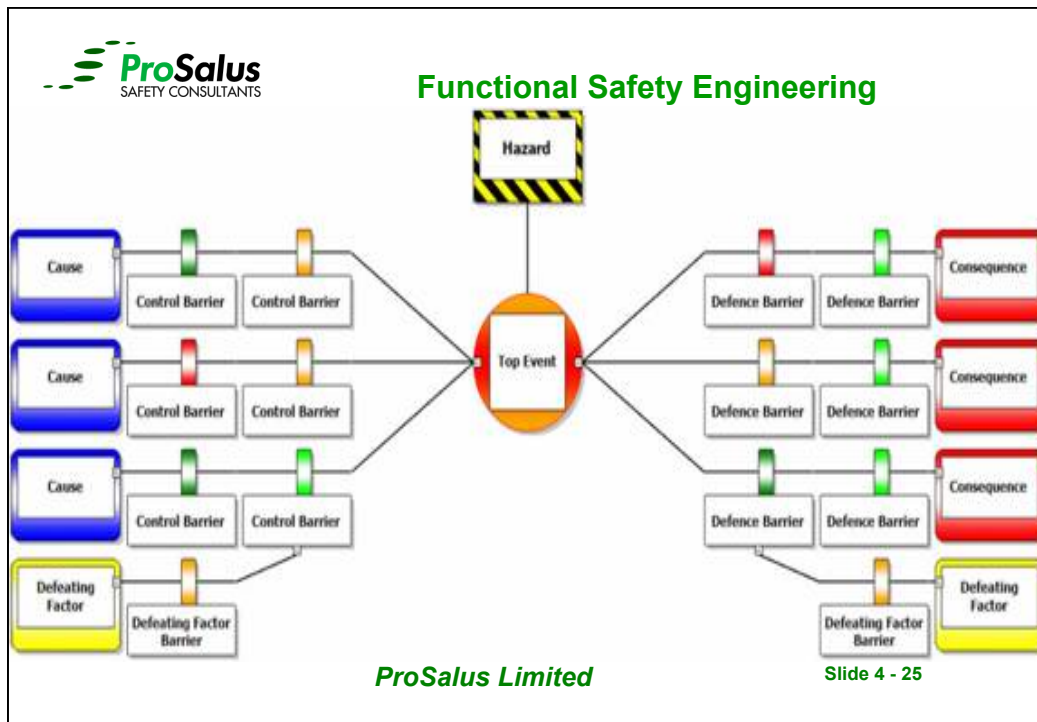
Slide 4 - 22




 **Functional Safety Engineering**

- **Bow Tie Diagram**
 - Simple Graphical means to illustrate the relationship between
 - Major risk / hazard / undesirable event
 - Its causes / threats
 - Its consequences
 - The associated prevention and mitigation controls
 - Helps demonstrate how major risks are controlled
 - Supports the Safety case
 - Can be Qualitative or Semi Quantitative

ProSalus Limited Slide 4 - 24



 **Functional Safety Engineering**

IEC 61511
Safety Allocation
and
Risk Reduction Analysis Techniques

ProSalus Limited Slide 4 - 26



Functional Safety Engineering

Introduction to Risk Reduction

- Risk Reduction can be achieved through any of the techniques which impact on the reduction of risk
- Risk can be spread across several techniques usually termed safety allocation:
 - Process design – focus's on inherent safety;
 - Technical Safety – focus's on passive protection measures
 - Functional Safety – focus's on active protection measures
 - Procedures & Process Safety Management
- All of these activities can form a part of the ALARP argument

ProSalus Limited

Slide 4 - 27



Functional Safety Engineering

Impact of Risk Reduction Techniques

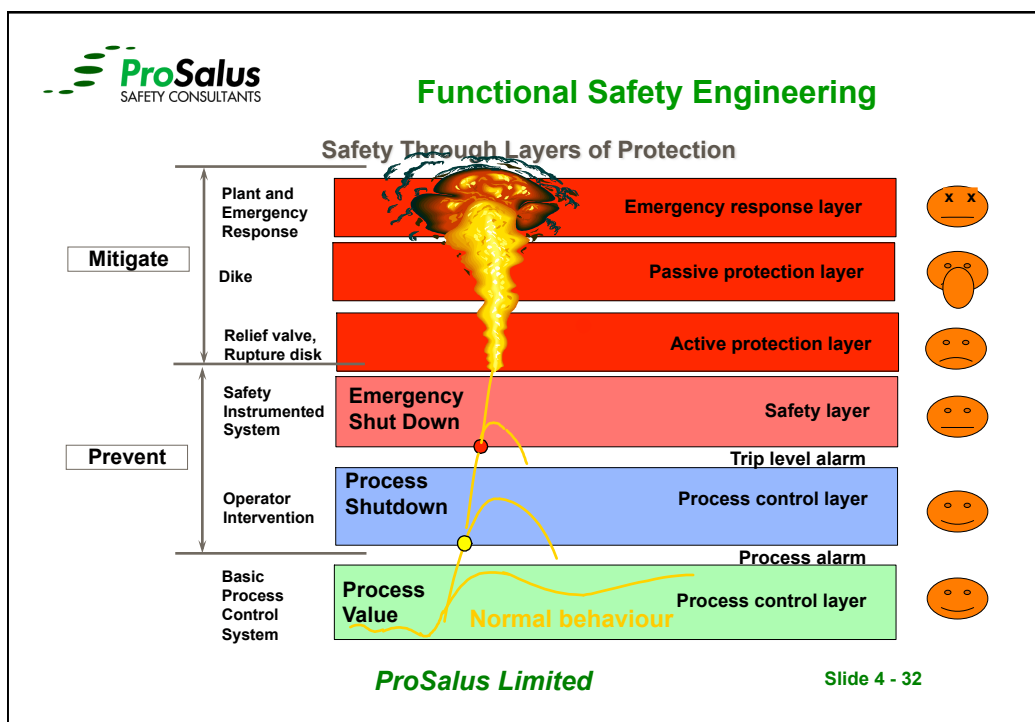
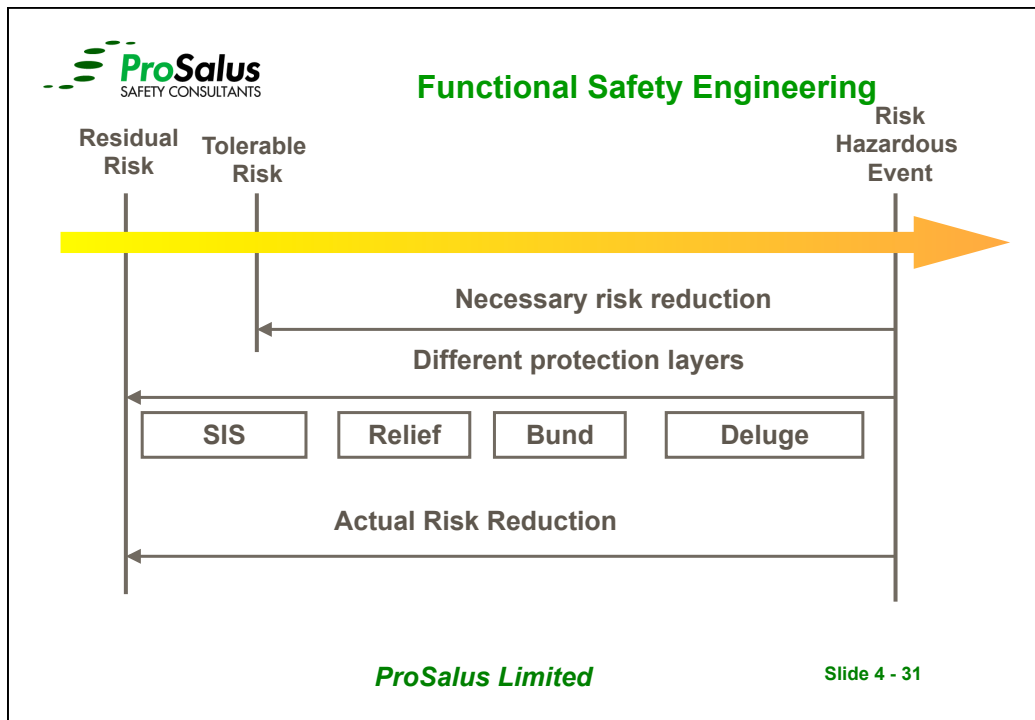
- Process design – reduction in severity of consequences and frequency of occurrence factors
- Mechanical design – reduction in severity of consequences and frequency of occurrence factors
- Layout design - reduction in severity of consequences and frequency of occurrence factors
- Control System design - frequency of occurrence factors
- Alarms - frequency of occurrence factors
- SIS design - frequency of occurrence factors
- F&G design - reduction in severity of consequences

ProSalus Limited

Slide 4 - 28

- **Risk Reduction Analysis techniques can be:**
 - Qualitative: everything expressed in words
 - Quantitative: everything expressed in numbers
 - Semi- quantitative: a mixture of words and numbers

- **IEC 61511 Risk Reduction Analysis techniques**
 - Simplified Risk Models
 - Fault tree analysis (FTA)
 - Event tree analysis (ETA)
 - Layer of protection analysis (LOPA)





Functional Safety Engineering

Simplified Risk Reduction Terms and Equations for use in Low Demand mode Applications

Ft = Tolerable Risk Frequency
 Fnp = Unprotected Risk Frequency
 Fp = Protected Risk Frequency

The Risk Reduction Factor:
 $RRF = F_{np} / F_t$

Safety Availability:
 $SA\% = (RRF - 1) \times 100 / RRF$

Probability of Failure on Demand:
 $PFD_{avg} = 1 / RRF = \Delta R = F_t / F_{np}$

ProSalus Limited

Slide 4 - 33



Functional Safety Engineering

Example of Simple Risk Matrix Table

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	minor injury	prod loss
1 per year	I	I	I	II
1 per 10 years	I	I	II	III
1 per 100 years	I	II	III	III
1 per 1000 years	II	III	III	IV
1 per 10000 yrs	III	III	IV	IV
1 per 100000 yrs	IV	IV	IV	IV

ProSalus Limited

Slide 4 - 34



Functional Safety Engineering

Example of applying the Risk Matrix Technique

A chlorine electrolyser plant presents a major leak hazard due to loss of pressure control.

The estimated frequency of occurrence is once per 10 years.

The estimated consequence without any protective measures is that the operating team of 3 people will be likely to suffer serious injury or they may be killed.

ProSalus Limited

Slide 4 - 35



Functional Safety Engineering

Use the information given above and the Risk Matrix table below to classify the given risk and its frequency

Using this table, decide the maximum tolerable risk frequency to reduce the risk to class 3 (considered to be acceptable)

Calculate the target risk reduction factor, PFDavg values and safety availability required from the proposed Safety Instrumented System to achieve the tolerable risk frequency

State the target safety integrity level required from the SIS by reference to the SIL tables

ProSalus Limited

Slide 4 - 36

Example of Risk Matrix Table

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	minor injury	prod loss
1 per year	I	I	I	II
1 per 10 years	I	I	II	III
1 per 100 years	I	II	III	III
1 per 1000 years	II	III	III	IV
1 per 10000 yrs	III	III	IV	IV
1 per 100000 yrs	IV	IV	IV	IV

ProSalus Limited

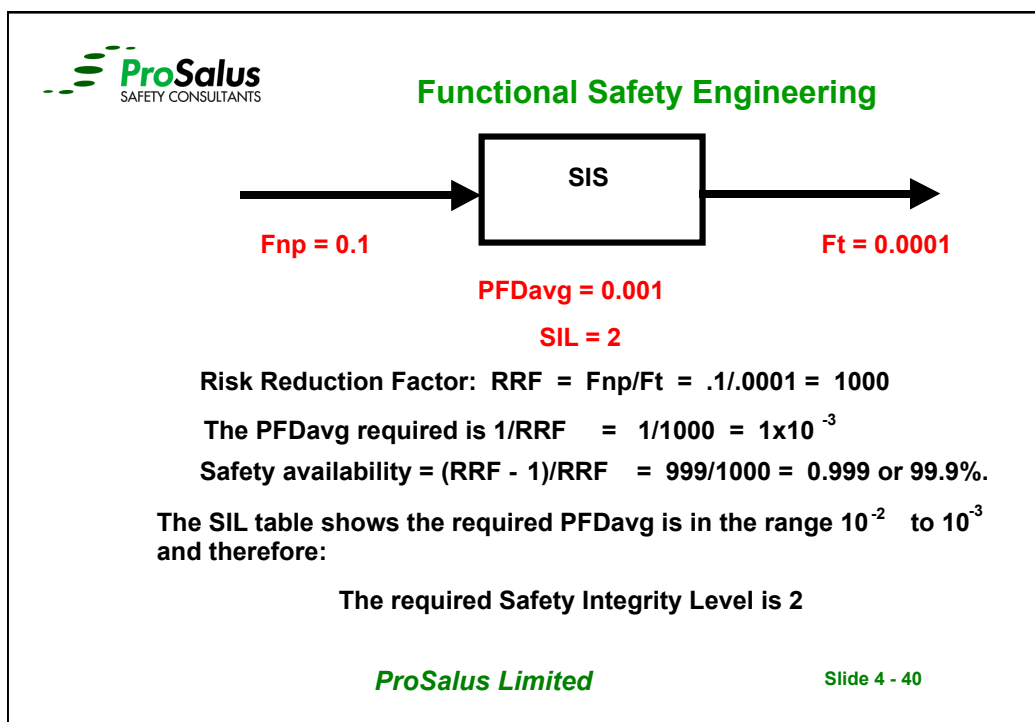
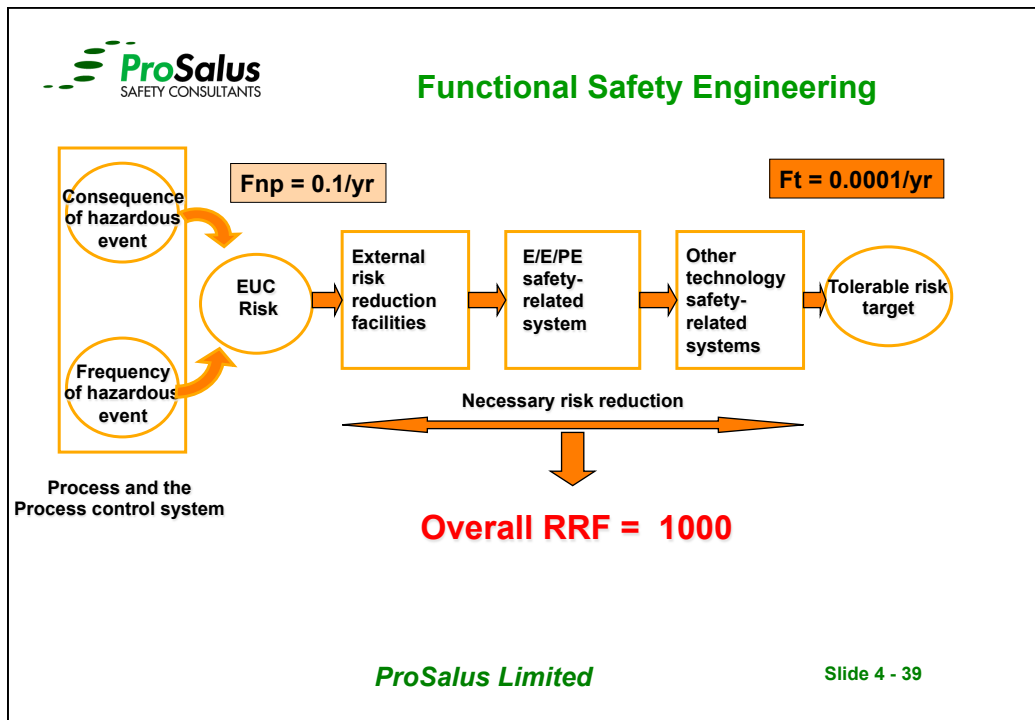
Slide 4 - 37

Example of Risk Matrix Table

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	minor injury	prod loss
1 per year	I	I	I	II
1 per 10 years	I	I	II	III
1 per 100 years	I	II	III	III
1 per 1000 years	II	III	III	IV
1 per 10000 yrs	III	III	IV	IV
1 per 100000 yrs	IV	IV	IV	IV

ProSalus Limited

Slide 4 - 38



Functional Safety Engineering

Safety Integrity Levels

Target failure measures (PFDavg) for a safety function operating in a low demand mode of operation

SIL	PFD	Safety Availability	Risk Reduction
4	0.0001 - 0.00001	0.9999 - 0.99999	10000 - 100000
3	0.001 - 0.0001	0.999 - 0.9999	1000 - 10000
2	0.01 - 0.001	0.99 - 0.999	100 - 1000
1	0.1 - 0.01	0.9 - 0.99	10 - 100

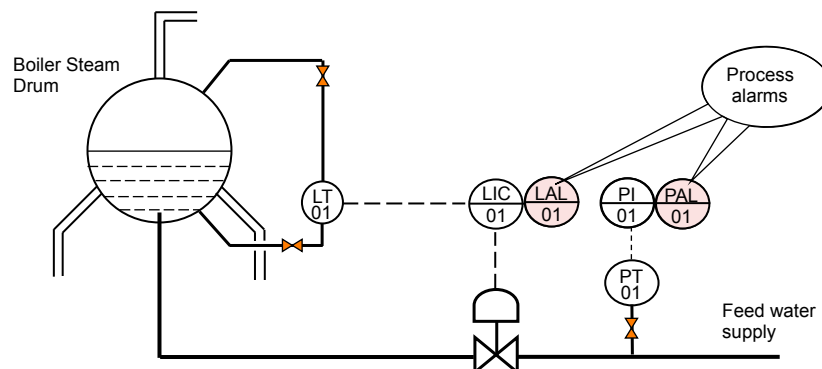
ProSalus Limited

Slide 4 - 41

Functional Safety Engineering

Example of applying a Simplified Risk Model

Target RRF Determined as = 1000



HAZOP Study has identified a hazard of low level in Boiler drum leading to possible tube rupture and potential burn injury or possible fatality of 1 person with a frequency of once per year.

ProSalus Limited

Slide 4 - 42



Example of Risk Matrix Table

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	minor injury	prod loss
1 per year	I	I	I	II
1 per 10 years	I	I	II	III
1 per 100 years	I	II	III	III
1 per 1000 years	II	III	III	IV
1 per 10000 yrs	III	III	IV	IV
1 per 100000 yrs	IV	IV	IV	IV

ProSalus Limited

Slide 4 - 43

Example of Risk Matrix Table

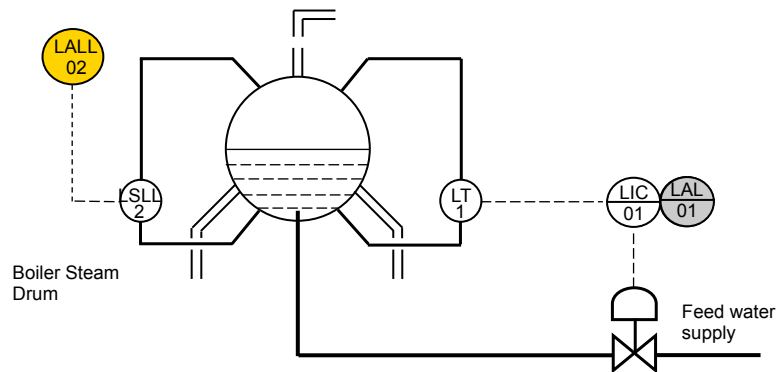
Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	minor injury	prod loss
1 per year	I		I	II
1 per 10 years	I		II	III
1 per 100 years	I		III	III
1 per 1000 years	II		III	IV
1 per 10000 yrs	III	III	IV	IV
1 per 100000 yrs	IV	IV	IV	IV

ProSalus Limited

Slide 4 - 44

Stage 1 – Consider an Independent Alarm Function

Low Low Level Alarm

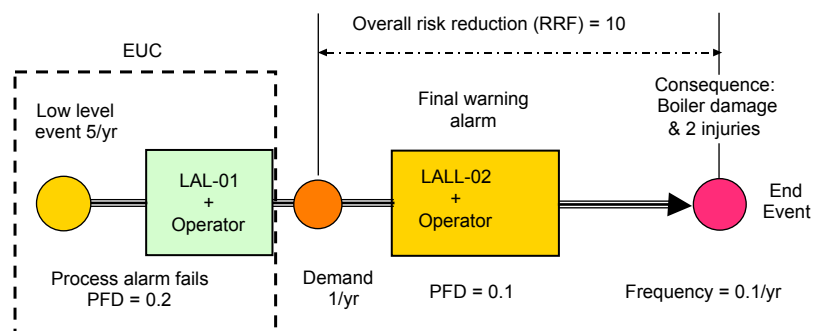


ProSalus Limited

Slide 4 - 45

Risk reduction model for Independent Alarm Function.

$$RRF = 1/PFD$$

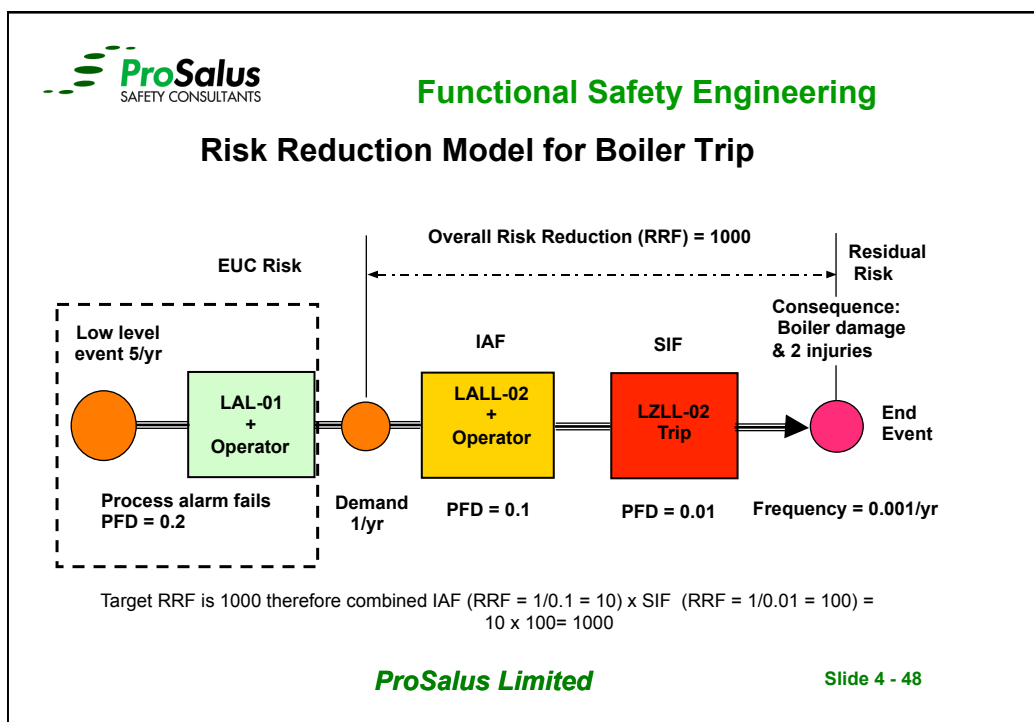
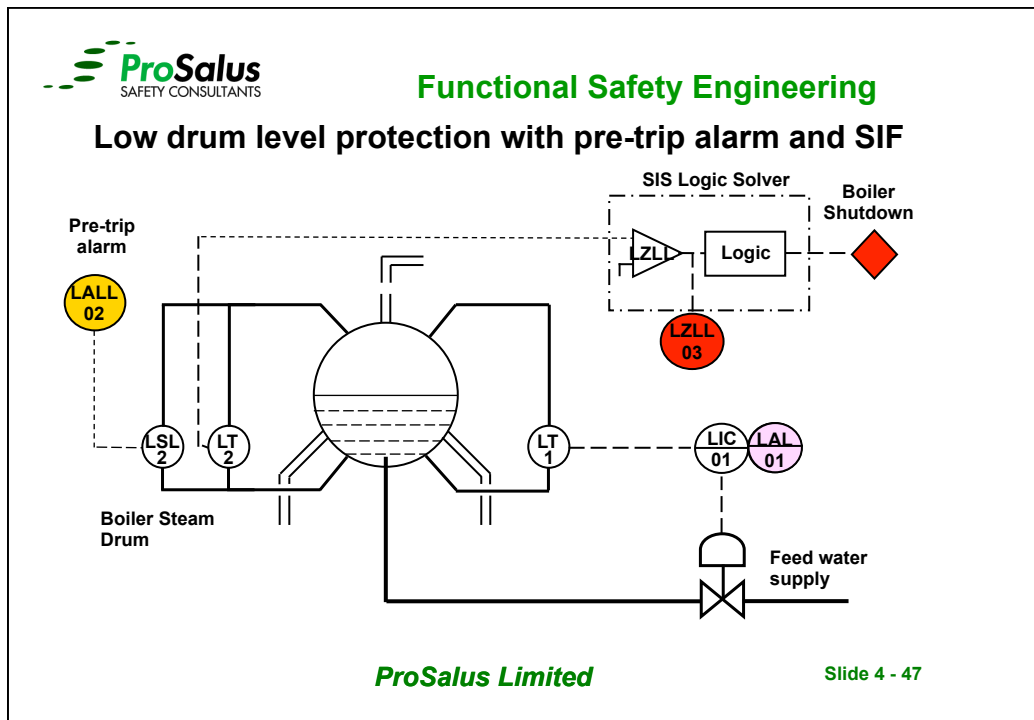


Low level in drum 5 times per year operator misses process LAL once per year, assume 1 demand on IAF per year.

We must consider operator as well and therefore limit alarm to 0.1 in line with IEC 61511-3 guidance

ProSalus Limited

Slide 4 - 46



- **Fault Tree Analysis**

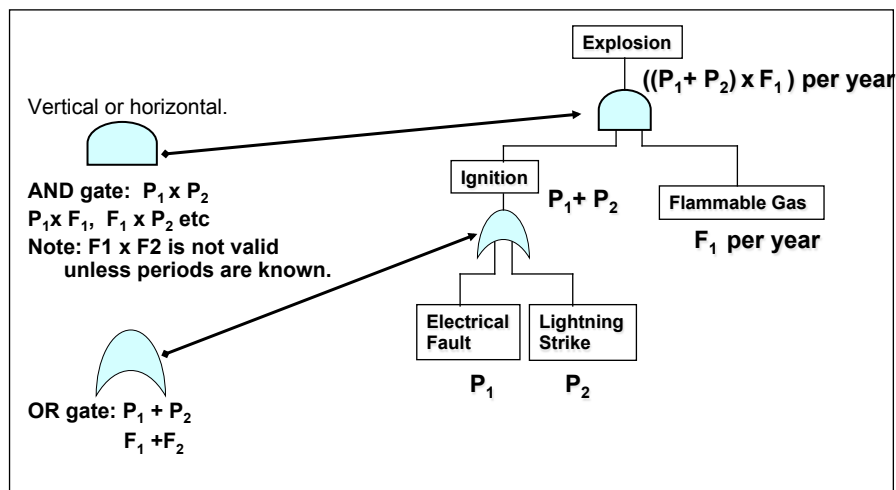
- It is a top down technique
- It starts with an undesired top event and from there we try to find out all different ways the top event can occur
- It can be used to find any combination of events or failures that can cause the TOP event
- It is a verification technique

- **What is fault tree analysis about?**

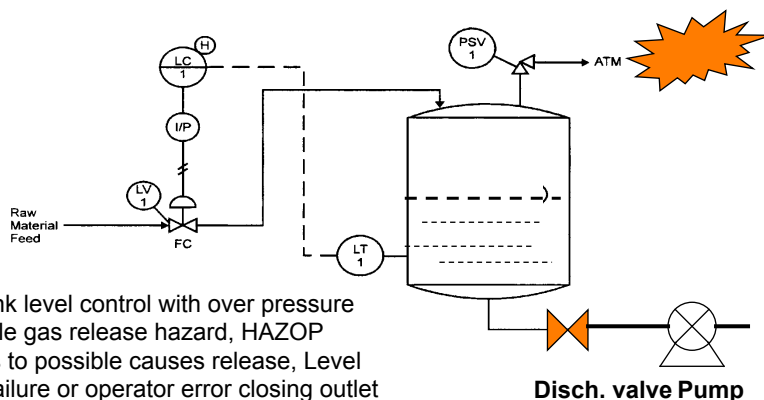
- The causes of the TOP event are connected through logic gates in a tree format
- Most common technique for casual analysis in risk and reliability studies, specially in the nuclear, aerospace and defence industries
- Can be performed qualitative as well as quantitative

■ The FTA Process

- Define scope of project
- Define the top event
- Develop the fault tree using gates
- Identify Cut Sets (combination of base events that can cause the top event to occur)
- Add Numerical values (Failures & Probabilities)
- Document results



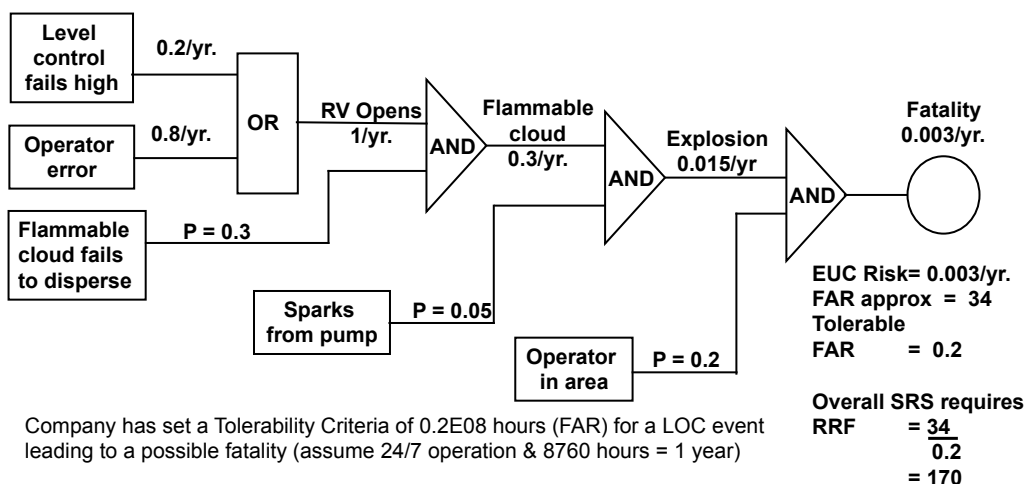
Example of applying Fault Tree Analysis to a Risk Reduction



ProSalus Limited

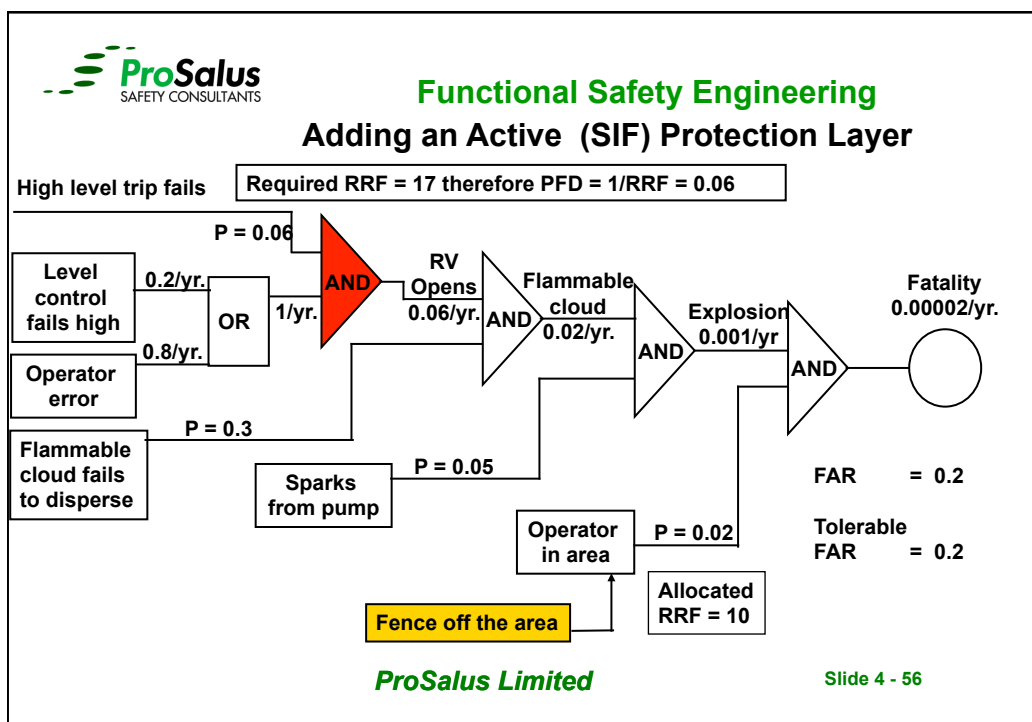
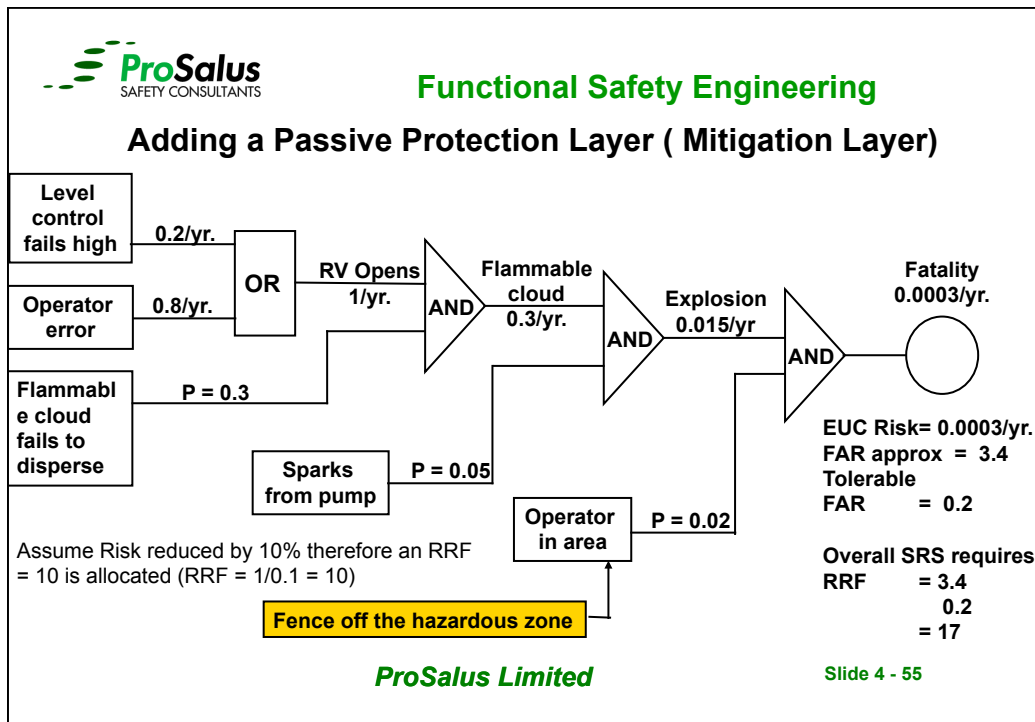
Slide 4 - 53

Fault Tree for Tank Loss of Containment Example



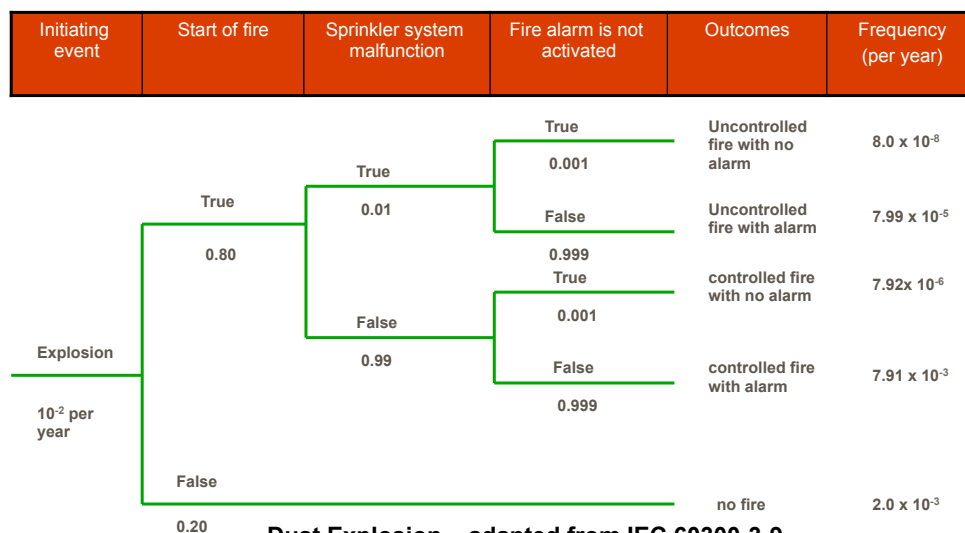
ProSalus Limited

Slide 4 - 54



■ Event Tree Analysis

- Helps us understand the consequences of events
- Models an initiating event and the time sequence of event propagation to the potential consequences
- Can be used qualitatively as well as quantitatively
- Can be developed independently or in combination with fault tree analysis

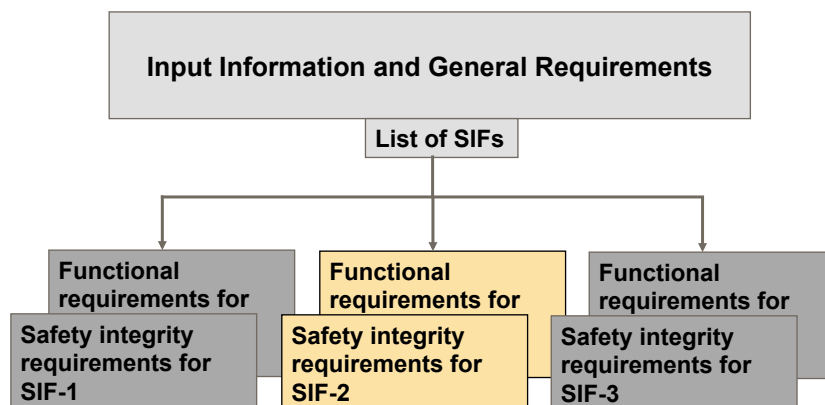


Dust Explosion – adapted from IEC 60300-3-9

Safety Requirements Specification

Slide 4 - 59

Safety Requirements Specification



ProSalus Limited

Slide 4 - 60



Functional Safety Engineering

Safety Integrity Requirements for a SIF

- The SIL of a SIF has been selected during the SIL determination study:
 - Risk Graph, LOPA, Risk matrix
 - SIL 1, 2 or 3
- This information must now be communicated to the design team to ensure the design meets the SIF safety integrity requirements during implementation
- This is communicated by the Safety Requirements Specification (SRS) which is the basis of the SIS validation

ProSalus Limited

Slide 4 - 61



Functional Safety Engineering

Functional Requirements for a SIF

- Functional requirements are derived from the hazard study and typically captured in the:
 - Piping & Instrument Diagrams
 - Cause & Effect Matrix
 - SIS Philosophy document
 - Functional Logic Diagram
- This information is communicated to the design team via the SRS to ensure required functionality is implemented
- This functionality is translated into the Functional design Specification (FDS) which is the basis of the SIS design

ProSalus Limited

Slide 4 - 62



Functional Safety Engineering

Safety Requirements Specification

- The SRS must be prepared before commencing any design work
- Be based on the guidance in IEC61511-1/2 Clause 10 & 12
- Expressed and structured in such a way that it is:
 - Clear;
 - Precise;
 - Verifiable;
 - Maintainable;
 - Feasible
- Written to aid comprehension by those who are likely to utilize the information at any phase of the lifecycle

ProSalus Limited

Slide 4 - 63



Functional Safety Engineering

Framework for the SRS

The SRS contains the functional and integrity requirements for each SIF and should provide sufficient information to design and engineer the SIS and include statements on the following for each SIF:

- Description of the SIF;
- Common cause failures;
- Safe state definition for the SIF;
- Demand rate;
- Proof test intervals;
- Response time to bring the process to a safe state;
- SIL and mode of operation (demand or continuous);
- Process measurements and their trip points;
- Process output actions and successful operation criteria;
- Functional relationship between inputs and outputs;

ProSalus Limited

Slide 4 - 64



Functional Safety Engineering

Framework for the SRS

- Manual shutdown requirements;
- Energizing or de-energizing to trip;
- Resetting after a shutdown;
- Maximum allowed spurious trip rate;
- Failure modes and SIS response to failures;
- Starting up and restarting the SIS;
- Interfaces between the SIS and any other system;
- Application software;
- Overrides / inhibits / bypasses and how they will be cleared;
- Actions following a SIS fault detection

Non-safety instrumented functions may be carried out by the SIS to ensure orderly shutdown or faster start-up. These must be separated from the SIFs.

ProSalus Limited

Slide 4 - 65



Functional Safety Engineering

Example SRS Template

SYSTEM REQUIREMENTS		Rev
SIF TITLE	HP KO Drum Overfill Protection System	
DESCRIPTION OF SIF	Close the feed valves to the HP KO Drum 43VD001 if 1oo2 level Instruments detect 84.8.7% level in 43VD001 and stops 2oo2 Seawater pumps.	04
P&ID No:	3203-T-VAB-P-XB-43-0020-01 & 3203-T-VAB-P-XB-50-0010-01	04
SCD No:	3203-T-VAB-I-XL-43-0020-01 & 3203-T-VAB-I-XL-50-0010-01	04
INSTRUMENT IDENTIFICATION	43LST0141A/B, 43LST0132 and 43LST0133	04
INSTRUMENT DESCRIPTION	43LST0141A/B: Gamma Pilot M FMG60 / AIM Safe	04
TRIP POINTS	43LST0141A/B: 84.8% level in 43VD001	04
ACTIONS / OUTPUTS	1) Stop 50PS001A 2) Stop 50PS001B	04
SUCCESS CRITERIA	Valves closed / Pumps stopped and prevented from being opened / restarted until the trip condition has been cleared and SIF is reset.	04
FUNCTIONAL RELATIONSHIP	43LST0141A/B: 1oo2 level Instruments detect 84.8% level in 43VD001, THEN stop 2oo2 Seawater pumps. AND prevents either Seawater pump from being started UNTIL the trip condition has been cleared and the SIF has been reset. If a diagnostic fault alarm is present on 2oo2 level Instruments, THEN stops 2oo2 Seawater pumps. AND prevents either Seawater pump from being started UNTIL the fault condition has been cleared and the SIF has been reset.	04
COMMON CAUSE FAILURES		
POWER LOSS	Upon power loss seawater pumps. If the logic solver is powered off, all the outputs are powered off breaking the power circuit to the pumps stopping them.	04
COMPRESSED AIR LOSS	Not Applicable.	04

ProSalus Limited

Slide 4 - 66

Example SRS Template

PROCESS DETAILS			
1	NORMAL PLANT OPERATION	There are no continuous sources to the HP KO Drum during normal operation, the drum has sufficient capacity for accumulation of liquid slugs up to 100m ³ in the subsea depressurisation mode between NLL and LAHH (PSD - 42.1%) all ESD valves are open and the seawater pumps are running.	
5	ABNORMAL PLANT OPERATION	Level is exceeded due to increase flow in condensation, from the oil system, separation system, relief from Heat exchangers or depressurisation of equipment	
3	SIS INTERFACES	An alarm is required to indicate that the SIF has been demanded i.e. If or 43LST0141A/B LAHH (ESD - 84.7%) has been exceeded. An alarm is required to indicate that any subsystem within the SIF has a diagnostic fault i.e. 43LST0141A/B has diagnosed an internal failure An inter trip from the OPS to ESD2 is required for a 43LST0141A/B LAHH (ESD - 84.7%) exceeded	04
7	SAFE STATE DEFINITION	50PS001A/B seawater pumps stopped and no cooling required.	04
3	CONCURRENT SAFE STATES CREATING A SEPARATE HAZARD	None identified	
3	PROCESS SAFETY TIME	Within 45 seconds for seawater pumps stop from LAHH - ESD detected (84.7%)	04
3	NORMAL OPERATIONAL PROCEDURES	Drum operates at 20% full with one seawater pump operational and cooling required	
1	ABNORMAL OPERATIONAL PROCEDURES	Drum operates at 65% full with one pump running and no cooling required	
2			

ProSalus Limited

Slide 4 - 67

Example SRS Template

SIL DATA					
3	TARGET SIL	TARGET	2	ACTUAL	2
1	TARGET SAFETY INTEGRITY	1.65E-03			
3	MODE OF OPERATION	Demand Mode			
3	SOURCES OF DEMAND	Level is exceeded due to increase flow in condensation, from the oil system, separation system, relief from Heat exchangers or depressurisation of equipment or the due to: 1) Maximum normal production 2) Choke Failure 3) Process depressurisation 4) Blocked outlet of Alvhheim Inlet Separator 5) Pressure Safety Valve or Rupture Disc 6) Blowdown of production flow lines 7) Spill off Control Valves 8) Manual Flare Valves 9) Leakage through valves and relief valves			
7	DEMAND RATE ON SIF (IF KNOWN)	TBC			
3	PROOF TEST INTERVAL	TARGET	3 Years	ACTUAL	3 years
3	SIS RESPONSE TIME	TARGET	Within 5 seconds	ACTUAL	2 seconds
3	SPURIOUS TRIP RATE	TARGET	1 per 10 years	ACTUAL	1 per 10 years
1	MEAN TIME TO REPAIR	4 hours			
2					

ProSalus Limited

Slide 4 - 68

Functional Safety Engineering Example SRS Template

0 TRIP ACTIONS			
3	OPERATOR INTERFACES	The operator will be able to monitor the SIF status and control the functions of the SIF by the use of a password via the HMI. Each input (including internal diagnostic fault alarm status) shall be provided with an alarm on the HMI that shall alert the operator when the input is in the tripped state irrespective of the override condition. An audible alarm will also be sounded. Operators can silence the sounder, and acknowledge the trip at the HMI. The trip is reset via the HMI and requires a password to initiate the reset once the trip condition has been cleared. This will allow the Seawater pumps to be restarted.	04
1	SYSTEM START/ RESTART	The trip system logic solver is implemented via a PLC, and while the PLC is powered, and the appropriate I/O is connected and powered, the system will monitor the HP KO Drum status. Upon power up, the SIF will be in the tripped state, and will need to be reset via the HMI, provided that neither a trip nor diagnostic fault condition is present. This will allow the pumps to be restarted.	04
5	MANUAL SHUTDOWN REQUIREMENTS	The existing ESD pushbutton system will remain unchanged and not be a direct input to the OPS.	
3	ENERGISE / DE-ENERGISE TO TRIP	LAHH from SIS is to de-energise interposing relay. The relay configuration is such that this energises a contactor which applies power to a switching mechanism to drive open the contacts to remove power from the pumps	04
7	RESETTING AFTER A SHUTDOWN	A trip is reset via the HMI and requires a password to initiate the reset, provided that the trip condition is no longer present. This will allow the pumps to be restarted.	04
3	OVERRIDES / INHIBITS / BYPASSES	A maintenance override is required for all input and outputs to facilitate on line maintenance and function testing of subsystems after maintenance and repair. The override will be via the HMI and will require a password to initiate the override. An alarm will be raised on the HMI to indicate that the override is present and the override time and name of the initiator will be logged by the event recorder. All maintenance overrides shall be password protected and in addition, any override that is left in over ride position for more than 8 hours will initiate a critical alarm	
9	DANGEROUS COMBINATIONS OF OUTPUT STATES	Both Sea water pumps stopped when heat exchangers still in use	
9	SPECIFY ACTIONS TO ACHIEVE / MAINTAIN SAFE STATE ON SIS FAULT INCLUDING HUMAN FACTORS	If there is a 2oo2 SIF diagnostic fault on the sensor sub systems or a 2oo2 diagnostic fault on the logic solver sub system, the plant will shutdown. If the fault occurs during a high high level condition then the general ESD push button should be initiated, in line with the current plant functionality.	04

ProSalus Limited

Slide 4 - 69

Functional Safety Engineering Example SRS Template

0 FAILURE MODES			
3	SENSOR FAILURES	43LST0141A/B are nucleonic detectors providing an analogue input to the PLC, the detector will be designed to fail safe i.e. A zero signal to the PLC, will result in a fault alarm. If all sensors (2oo2) are in a failed state the PLC will stop the seawater pumps	04
4	LOGIC SOLVER FAILURES	The PLC will be configured such that the safe state of the plant will be maintained if it is powered down or removed. i.e. No supply to the Seawater pumps, thus the pumps will stop. If there is a failure of the PLC, an alarm will be raised on the HMI. If there is a 2oo2 diagnostic fault on the PLC the system will shutdown with all outputs set to zero.	04
5	FINAL ELEMENT FAILURES	The pumps will be designed to fail stopped, and will only start if there is no trip condition. If the pump fails to stop on command or allows seawater to pass these are dangerous failures which will be taken into account in the SIL verification calculations. Pump discrepancy alarms will be raised on the HMI if the pump is running when commanded to stop or stopped when commanded to start.	04
3	DESIRED RESPONSE OF SIF TO FAILURE MODES	1) Stop 50PS001A 2) Stop 50PS001B	04
0 APPLICATION SOFTWARE			
3	SOFTWARE TYPE	Vendor SIL 3 TUV Certified module library	
9	SOFTWARE REQUIREMENTS TO CLAUSE 12.2.2 OF IEC 61511	3203-T-VAB-I-SR-43-0022-01	
0 ENVIRONMENTAL EXTREMES			
1	TEMPERATURE	+/- 20 degrees Celsius	
2	HUMIDITY	Up to 85%	
0 MAINTENANCE ISSUES			
3	CONSIDERATIONS	Routine testing and maintenance will be implemented when the plant is shut down. Breakdown maintenance can be done by utilising the maintenance override for the channel under repair and by replacement of faulty components.	
1.0 NOTES			

ProSalus Limited

Slide 4 - 70

Fault Tree Analysis Exercise

Practical exercise no: 1 Fault Tree Analysis

This practical exercise requires attendees to construct a fault tree diagram using the basic principles introduced in this module. It uses an example of a simple reactor with automatically controlled feeds that has the potential to cause a serious risk to plant personnel.

Once the basic fault tree has been drawn, the model is to be adjusted to incorporate a safety-instrumented system and to demonstrate the resulting risk reduction.

The process is a reactor with a continuous feed of fuel and oxidant. Two flow control loops are operated under a ratio controller set by the operator to provide matching flows of fuel and oxidant to the reactor. An explosive mixture can occur within the reactor if the fuel flow becomes too high relative to the oxidant flow.

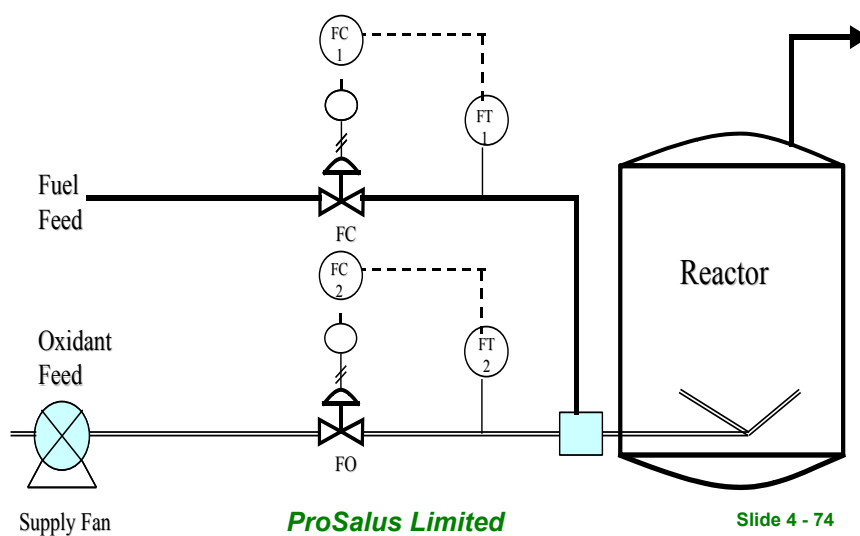
Possible causes are: Failures of the BPCS or an Operator error in manipulating the controls leading to sudden loss of oxidant feed.

A SIS is proposed with a separate set of flow meters connected to a flow ratio measuring function that is designed to trip the process to safe condition if the fuel flow exceeds the oxidant flow by a significant amount

The tag number for this Safety Instrumented function is FFSH- 03

ProSalus Limited

Slide 4 - 73



ProSalus Limited

Slide 4 - 74

